UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/042,652	01/08/2002	Jeffrey Bruce Lotspiech	ARC920010090US1	7388

7590 10/24/2005

John L. Rogitz
Rogitz & Associates
750 B Street, Suite 3120
San Diego, CA 92101

EXAMINER	
BERGER, AUBREY H	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 10/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/042,652	LOTSPIECH ET AL.	
	Examiner	Art Unit	
	Aubrey H. Berger	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 January 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *01/08/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-48 are pending.

Priority

2. This application repeats a substantial portion of prior Application No. 09/770,877, filed January 26, 2001, and adds and claims additional disclosure not presented in the prior application. Since this application names an inventor or inventors named in the prior application, it may constitute a continuation-in-part of the prior application. Should applicant desire to obtain the benefit of the filing date of the prior application, attention is directed to 35 U.S.C. 120 and 37 CFR 1.78.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on January 26, 2002 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Drawings

4. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "18" has been used to designate both "compliance enforce" and "subscription enforce". Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either

"Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

5. The disclosure is objected to because of the following informalities:

a. "Block 20" is recited on page 11, line 13 and is not represented in the drawings and is believed to represent the block titled "subscription enforce".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Number 6,691,149 to Yokota et al (Yokota).

Regarding claim 1, Yokota discloses a method for securely transmitting multicast data (col. 5, lines 37-42), comprising: encrypting at least one title T/content, with at least title key K_T/contents key, and encrypting the title key K_T/contents key, with at least one channel-unique key K_{cu}/storage key (col. 9, lines 33-37), using at least one encryption function S/DES (col. 9, lines 14-16), to render a multicast data channel encrypted as $S_{Kcu}(K_T)$, $S_{KT}(T)$, (fig. 1, # 22).

7. Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication Number 2001/0029581 to Knauft.

Regarding claim 1, Knauft discloses a method for securely transmitting multicast data comprising: encrypting at least one title T/data object, with at least title key K_T /symmetric session key, and encrypting the title key K_T/symmetric session key (fig. 5A, #502), with at least one channel-unique key K_{cu}/public program key (fig. 5A, #504), using at least one encryption function S, to render a multicast data channel encrypted as $S_{Kcu}(K_T)$, $S_{KT}(T)$, (fig. 5A, #514).

8. Claims 1, 23-26, and 41-46 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Number 6,690,795 to Richards.

Regarding claim 1, Richards discloses a method for securely transmitting multicast data (fig. 1), comprising: encrypting at least one title T/program A (fig. 2, #2), with at least title key K_T /Segment Key (fig. 2, #2), and encrypting the title key K_T/Segment Key, with at least one channel-unique key K_{cu}/Customer_code (fig. 2), using at least one encryption function S/DES (col. 6, lines 8-10), to render a multicast data channel encrypted as $S_{Kcu}(K_T)$, $S_{KT}(T)$, (fig. 2, #9).

Regarding claim 24, Richards discloses a method for enforcing copy protection compliance and subscription compliance comprising: providing players with respective device keys K_d/customer code, useful for enabling copy protection compliance, and providing players with at least one channel key K_c/working key (control channel key), useful for enabling subscription compliance such that a player can decrypt content only if the player is both compliant with

copy protection and the player is an active subscriber to a content channel (col. 4, lines 43-46; fig. 27 & 28).

Regarding claims 23 and 25, Richards discloses wherein the content is streamed to players (col. 2, lines 41-43).

Regarding claim 26, Richards further discloses the method of claim 25, comprising: encrypting at least one title T/program A (fig. 2, #2), with at least title key K_T /Segment Key (fig. 2, #2), and encrypting the title key K_T/Segment Key, with at least one channel-unique key K_{cu}/Customer_code, using at least one encryption function S/DES (col. 6, lines 8-10), to render a multicast data channel encrypted as $S_{Kcu}(K_T)$, $S_{KT}(T)$, (fig. 2, #9).

Regarding claim 41 and 43, Richards discloses a player/system, for decrypting streamed content (col. 2, lines 42-44; col. 1, lines 21-23), comprising: at least one device key K_d/customer code, means for decrypting a session key K_s/segment key, using the device key K_d/customer code, means for decrypting a channel unique key K_{cu}/channel access key, using at least the session key K_s/segment key, and means for deriving a title key K_T/program key, using at least the channel unique key K_{cu}/channel access key, the title key K_T/program key, being useful for decrypting content (fig. 17).

Regarding claim 42, Richards discloses the player/system, of claim 41, wherein the content is multicast to the player (col. 1, lines 13-18).

Regarding claim 44, Richards discloses a computer program device comprising: a computer program storage device including a program of instructions usable by a computer (col. 2, line 63), comprising: logic means for

receiving private information I_u/header (fig. 1, #2), upon registration with a content provider, logic means for subscribing to at least one content channel provided by the content provider (col. 3, lines 7-12), logic means for receiving at least one encrypted channel key K_c/control channel key (fig. 14), at least partially in response to subscribing to the channel, logic means for deriving the channel key K_c/control channel key, using the information I_u/header, and logic means for using at least the channel key K_c/control channel key, to decrypt content streamed over the channel (fig. 14).

Regarding claim 45, Richards discloses the computer program device of claim 44, further comprising: plural device keys K_d/customer code, logic means for receiving at least one session key block/DES (col. 21 lines 31-32), logic means for deriving at least one session key K_s/segment key, from the session key block using at least one device key K_d/customer code (fig. 8, #58).

Regarding claim 46, Richards discloses the computer program device of claim 45, further comprising: logic means for using the session key K_s/segment key, and channel key K_c/control channel key, to derive a channel unique key K_{cu}/channel access key, and logic means for using the channel unique key K_{cu}/channel access key, to decrypt a title key K_T/program key, useful for decrypting the content (fig. 27 & 28).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to

> be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 2-16, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over either Yokota, Knauft, or Richards as individually applied to claim 1 above, and further in view of U.S. Patent Application Publication Number 2002/0083319 to Ishiguro et al (Ishiguro).

Yokota, Knauft, and Richards lack a channel-unique key that is a result of a combination of a concatenation of the channel key and session key.

Regarding claims 2-3, Ishiguro teaches wherein the channel-unique key K_{cu}/e, is the result of a combination of a channel key $K_c/e1$, and a session key $K_s/e2$, wherein the combination is a hash function of a concatenation of the channel key $K_c/e1$, and session key $K_s/e2$, (¶ [0104]). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of either Yokota, Knauft, or Richards with the device of Ishiguro. One of ordinary skill in the art would have been motivated to perform such a modification to the device of Yokota, Knauft, or Richards because Ishiguro teaches the channel-unique key K_{cu}/e, can be obtained (and the content decrypted) only by a player that is compliant with both copy protection rules and subscription rules (abstract & fig. 4).

Regarding claim 4, Yokota, Knauft, or Richards further disclose the method of claim 2 as modified above, wherein the session key $K_s/e2$, is encrypted with at least a first encryption scheme B^R_{s1}/DES [Ishiguro, ¶ [0079], to render a session key block/sk2' (Ishiguro, ¶ [0105]).

Regarding claim 5, Yokota, Knauft, or Richards further disclose the method of claim 4 as modified above by Ishiguro, comprising providing at least one player with device keys K_d/license key (Ishiguro, fig. 4), to activate the player [Ishiguro, ¶ [0065]).

Regarding claim 6, Yokota, Knauft, or Richards further disclose the method of claim 5 as modified above by Ishiguro, comprising providing the player with the channel key K_c/e1 (Ishiguro, fig. 6).

Regarding claim 7, Yokota, Knauft, or Richards further disclose the method of claim 6 as modified above by Ishiguro, wherein at least one of the providing acts is undertaken in a point-to-point communication (Ishiguro, fig. 1).

Regarding claim 8, Yokota, Knauft, or Richards further disclose the method of claim 6 as modified above by Ishiguro, wherein at least one of the providing acts is undertaken as part of a broadcast (Ishiguro, ¶ [0105]).

Regarding claim 9, Yokota, Knauft, or Richards further disclose the method of claim 6 as modified above by Ishiguro, comprising providing the player with the session key block/sk2' (Ishiguro, fig. 6).

Regarding claim 10, Yokota, Knauft, or Richards further disclose the method of claim 9 as modified above by Ishiguro, wherein the player can determine the session key K_s/e2, from the session key block/sk2', using the device keys K_d/license key (Ishiguro, ¶ [0105]).

Regarding claim 11, Yokota, Knauft, or Richards further disclose the method of claim 10 as modified above by Ishiguro, comprising periodically

refreshing the channel key K_c/e1, (Ishiguro, fig. 7, steps 48-51) to enforce subscriptions.

Regarding claim 12, Yokota, Knauft, or Richards further disclose the method of claim 10 as modified above by Ishiguro, comprising selectively updating the session key block [Ishiguro, ¶0128].

Regarding claim 13, Yokota, Knauft, or Richards further disclose the method of claim 12 as modified above by Ishiguro, comprising updating the session key block/sk2', by encrypting an updated session key/e2, with at least the encryption scheme B^R_{s1}/DES (Ishiguro, ¶ [0079]).

Regarding claim 14, Yokota, Knauft, or Richards further disclose the method of claim 11 as modified above by Ishiguro, wherein a new channel key K_c'/e1, is encrypted with at least a second encryption scheme B^R_{s2}/n-bit block encryption (Ishiguro, ¶ [0241]).

Regarding claim 15, Yokota, Knauft, or Richards further disclose the method of claim 14 as modified above by Ishiguro, wherein the new channel key K_c'/e1, is sent in a message that is split (Ishiguro, fig. 7, steps 48-51).

Regarding claim 16, Yokota, Knauft, or Richards further disclose the method of claim 14 as modified above by Ishiguro, wherein the new channel key K_c'/e1, is refreshed using plural messages (Ishiguro, fig. 7, steps 48-51).

Regarding claim 47, Yokota, Knauft, or Richards further disclose the method of claim 14 as modified above by Ishiguro, wherein the new channel key K_c'/e1, is sent in-band with the title T (Ishiguro, fig. 7).

Ishiguro lacks partitioning players not in a revoked set R into disjoint subsets and encrypting the session key with the subset keys..

11. Claims 27-40 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Richards as applied to claims 24-26 above, and further in view of Ishiguro.

Regarding claim 27, Richards discloses the method of claim 26, and Ishiguro teaches wherein the channel-unique key K_{cu}/e, is the result of a combination of a channel key $K_c/e1$, and a session key $K_s/e2$, wherein the combination is a hash function of a concatenation of the channel key $K_c/e1$, and session key $K_s/e2$, (Ishiguro, ¶ [0104]). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Richards with the device of Ishiguro. One of ordinary skill in the art would have been motivated to perform such a modification to the device of Richards because Ishiguro teaches the channel-unique key K_{cu}/e, can be obtained (and the content decrypted) only by a player that is compliant with both copy protection rules and subscription rules (Ishiguro, abstract & fig. 4).

As per claims 28-37, 39-40, and 48 all claimed limitations have been addressed and/or cited as set forth above corresponding to claims 2-12, 15-16, and 48 respectively.

Regarding claim 38, Richards discloses the method of claim 35 as modified above by Ishiguro, wherein the new channel key $K_c'/e1$, is refreshed by encrypting a new channel key $K_c'/e1$, with at least one encryption scheme (Ishiguro, fig. 7, steps 48-51).

Double Patenting

12. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

13. Claims 1-22 provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 15-17 copending Application No. 09/770,877 in view of Yokota, Knauft, or Richards, in view of Ishiguro, and in further view of "Applied Cryptography" by Schneier.

b. Claims 15-17 is substantially equivalent to claims 17-22 of the instant application, except for the additional subject matter recited in claims 1-16. However, as described above, Yokota, Knauft, or Richards teaches these limitations are obvious. Further instant claims 17-22 recite B^{R}_{s2} which is not present in the prior application. However, Schneier teaches DES is a common form of block encryption and would be obvious to one of ordinary skill at the time the invention was made (page 270, 12.2)

This is a provisional obviousness-type double patenting rejection.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

c. U.S. Patent Application Publication 2005/0198679 is cited for teaching a conditional access method and apparatus for use with a system for controlling digital TV.

d. U.S. Patent Number 6,839,436 is cited for teaching broadcast encryption method that adapts to the presence of compromised keys and continues to broadcast securely to privileged sets of users over time.

e. U.S. Patent Application Publication Number 2005/0131832 is cited for teaching two authentication processes to protect content from access by an unauthorized user.

f. U.S. Patent Application Publication Number 2003/0051151 is cited for teaching a title unique key generated from its own keys, such as master, media and LSI keys based on the stored title key.

g. U.S. Patent Application Number 2002/0174366 is cited for teaching enforcement of content rights and conditions for multimedia content.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aubrey H. Berger whose telephone number is (571)272-8155. The examiner can normally be reached on Monday - Thursday, 7:30 a.m. - 5:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AHB

AHB

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100